UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

Civil Case No. 14-cv-1280

{Plaintiff} Malibu Media LLC

Plaintiff,

v.

{Defendant}John Doe subscriber assigned
IP address 69.249.253.94
"johndoe69249@hushmail.com"

DEFENDANT'S MOTION FOR PROTECTIVE ORDER REGARDING DEFENDANT'S COMPUTER HARD DRIVE(S)

Defendant John Doe ("Defendant") is identified in Plaintiff's complaint as the Internet Service Provider (ISP) subscriber assigned Internet Protocol ("IP") address 69.249.253.94. I am representing myself *pro se* in this matter before the Court. I understand that *pro se* litigants are required to follow the same rules and procedures as litigants that are represented by attorneys as seen in *Nielson v. Price,* 17 F.3d 1276, 1277 (10th Cir. 1994). I will abide by these rules and procedures, but ask the courts indulgence as I'm not a lawyer. I hereby bring this Motion, pursuant to Fed. R. Civ. P. 26© for a Protective Order regarding the information on my computer hard drive(s).

Specifically, and as detailed in the accompanying brief in support, the information on Defendant's hard drive(s) is personal and confidential in nature, and because most or all of that information is irrelevant to the issues in this case, and because of the nature of Plaintiff and its industry-scale litigation and settlement practices, Defendant wants the moral equivalent of an in camera inspection of his computer's hard drive, by using a licensed but neutral expert in computer forensics (paid for by the Plaintiff) who can provide the information to both parties

that is relevant to Plaintiff's claims, but who will not otherwise divulge the contents of the Defendant's computer to Plaintiff or anyone else.

WHEREFORE, Defendant respectfully requests a protective order from this Court limiting Plaintiff's discovery of Defendant's computer hard drive(s) to the procedures described in the accompanying supporting brief.

DATED: *September 30th*, 2014

Respectfully submitted,

By: 

John Doe
Pro se
johndoe69249@hushmail.com

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

Civil Case No. 14-cv-1280

{Plaintiff} Malibu Media LLC

Plaintiff,

v.

{Defendant}John Doe subscriber assigned
IP address 69.249.253.94
"johndoe69249@hushmail.com"

BRIEF IN SUPPORT OF DEFENDANT'S MOTION FOR PROTECTIVE ORDER

REGARDING DEFENDANT'S COMPUTER HARD DRIVE(S)

STATEMENT OF FACTS

Pending before this Court is an action for direct copyright infringement, under 17 U.S.C. 501, by Plaintiff, Malibu Media LLC ("Malibu") against Defendant John Doe subscriber assigned IP Address 69.249.253.94 ("Defendant").

Malibu is in the business of producing and distributing pornographic movies and, in cooperation with a German IT firm known (at least in this lawsuit) as IPP International UG ("IPP"), is also a prolific, for-profit copyright infringement litigator that has, since 2012, filed over 1800 copyright infringement suits involving alleged peer-to-peer file sharing. Meanwhile, Defendant is a self-employed computer technician in his late fifties who has never used BitTorrent or any of the services mentioned by Malibu in this case, because of all of them present a potential security risk. Indeed, Defendant only knows BitTorrent due to removal of infected versions through work as a computer technician and has never installed or used it on the computers that he owns. The Defendant has checked his computer for the presence of any of the files mentioned in Malibu's complaint, and has come up with nothing. Defendant has also checked for the presence of any BitTorrent or peer-to-peer distribution programs in his computer(s) and also came up with nothing. Defendant has not deleted or attempted to cover up anything, an expert in computer forensics would be able to tell whether there was any evidence of data destruction or spoliation upon examining Defendant's hard drive(s).

Presently at issue before this Court is a controversy about the examination of the hard drive(s) on Defendant's computer(s). Understandably, given the nature of its case, Plaintiff wants to examine Defendant's hard drive(s) in an effort to obtain evidence supporting its accusations that Defendant has used BitTorrentto directly infringe on the copyrights of their

pornography. Presumably, the Plaintiff would look for the BitTorrent program, BitTorrentfiles, or any usage of peer-to-peer file sharing, and any presence of the allegedly infringed works. With Malibu's usual investigator, Patrick Paige, and in order to facilitate its desire to dig around in the Defendant's computer, Plaintiff has always proposed, in past examples, to have its paid expert spend up to an entire business day making an exact duplicate (image) of the hard drive on the defendant's computer, and thereafter have its expert spend "weeks if not months" conducting an investigation of the image.

From the defendant's perspective, this procedure that is standard for the Plaintiff is needlessly invasive and lacks adequate safeguards, among other problems. In truth, Defendant welcomes the opportunity to demonstrate that he did not engage in peer-to-peer file sharing of Plaintiff's works, and fully expects the forensic examination of hi computer(s)' hard drive(s) will bear witness to that fact. However, the Defendant's computer holds a number of private documents and records that may include records of banking transactions, bank account numbers, tax records, social security numbers, mortgage payments, credit scores, income and financial worth, school and medical records, and all types of passwords to various accounts, as well as private communications that were never intended to be revealed to third persons.

Understandably, Defendant distrusts the particular persons who want to subject his confidential information to such exacting scrutiny. Defendant does not have the resources to monitor Malibu or IPP and hold them accountable, should they violate the protective order contemplated by Plaintiff. The Defendant would essentially have to trust them, yet time and time again pornographers with an industry-sized litigation practice of coercing settlements from blameless individuals do not provide the necessary confidence for such trust. Neither does the alleged data log from a foreign IT company that may be a shell for a previously discredited firm

(IPP may be a new shell for a pre-existing, but already known discredited German company named Guardley Limited) warrant such trust. While the Plaintiff may have absolute confidence in its own bona fides, one must remember that the Defendant ***knows*** that he did not infringe on Plaintiff's copyrights and, therefore he ***knows*** that the Plaintiff is the kind to sue innocent people and attempt (from his prospective) to extort money from them by drawing out the litigation process with numerous time extensions to rack up attorney fees on both sides.

Further, the Defendant lacks the funds to pay for his own forensic examination of his computer(s)'s hard drive(s). As outlined in the answers to Plaintiff's first set of interrogations, there are 4 computers to examine, each with multiple hard drives as well as external USB memory sticks. The Defendant reasonably fears that an unlicensed imaging "expert" could plant or what exculpatory evidence might be withheld by the Plaintiff's forensic examiner in an effort to squeeze him for money. Since the imagine and examination would not have to be done twice if the Defendant could trust both the results and have access to the same results as the Plaintiff, the procedures that the Defendant proposes is far superior to that proposed by the Plaintiff.

Finally, some accommodation must be made for the fact that what the Plaintiff is proposing will itself constitute (or may constitute) one or more violations of law. That is on the Defendant's computers are many copyrighted works, such as programs that the Defendant is legally licensed to use. It would be ironic is the Defendant is forced to actually abet copyright infringement in order to demonstrate that he had not previously done so. Pennsylvania law requires a proper license to conduct investigations for a fee. There for the individual paid to examine defendant's computer should be licensed in Pennsylvania, not Mr. Patrick Paige, the Plaintiff's usual investigator, who is located in Boynton Beach, FL.

ARGUMENT

I. THIS COURT SHOULD ENTER A PROTECTIVE ORDER THAT LIMITS THE DISCOVERY OF THE CONTENTS OF THE DEFENDANT'S COMPUTER(S) AND HARD DRIVE(S) TO AN EXAMINATION BY A LICENSED IN PENNSYLNIVA AND INDEPENDENT EXAMINER WHO CAN THEN DISCLOSE THE NECESSARY RELEVANT INFORMATION TO BOTH PARTIES IN ACCORDANCE WITH THE PROCEDURE PREVIOUSLY PROPOSE BY THE DEFENDANT.

Fed. R. Civ. P. 26(c)(1), in relevant part, provides that"[t]he court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense" Such an order may include "(A) forbidding the disclosure or discovery; (B) specifying the terms … for the disclosure or discovery; (C) prescribing a discovery method other than the one selected by the party seeking discovery …" *Id.* The decision to issue a protective order is left to "the broad discretion of the district court in managing the case." *Lewlling v. Farmers Ins. Of Columbus, Inc.*, 879 F.2d 212, 218 (6th Cir. 1989).

When weighing in the respective burdens, as discussed earlier, the Plaintiff wants to make a complete copy of everything stored on the Defendant's hard drive, and then have its paid examiners go through their usual process of spending weeks or possibly months poring over what they find there. The Defendant is of the position that nothing found on his computer(s)'s hard drive(s) will have any relevance to this case, except for that conclusion, that there is nothing relevant to this case there. Because the Defendant has no desire to let all the details of his personal and confidential information be scrutinized indefinitely by pornographers who (in his view) are engaging in a for-profit campaign of mass extortion through abuse of the litigation system; the Defendant has made a very reasonable proposal as to how the Plaintiff could obtain the information in which it has a legitimate interest that is outlined below.

Defendant's Proposal:

The defendant reasonable objects to a request for a production of a copy of all hard drives and external hard drives as this request imposes on the Defendant an annoyance, embarrassment, oppression, or undue burden or expense. Specifically, the Defendant does not have the personal skills or knowledge to produce such a copy, and should not be expected to bear the financial burden of hiring an expert to produce such a copy. More importantly, the hard drive(s) of the Defendant's computer(s) contain private and confidential information that is completely unrelated to any legitimate purpose of the Plaintiff in the instant lawsuit, and the Defendant should not be compelled to entrust such private and confidential matters to the custody and control of a pornographer/plaintiff. However, examination of the hard drive(s), within reason, is a necessary step to proceed with the case to show that the Defendant is innocent, so the Defendant proposes to allow the Plaintiff access to the information it seek as follow:

Plaintiff and Defendant shall mutually agree upon the selection of an independent expert in "computer forensics" who is properly licensed in Pennsylvania. If the Plaintiff and Defendant cannot agree on the selection of such an expert, then one shall be selected by the Court. The Defendant will bring his computers and external storage devices in for inspection by the independent computer forensics expert.The said expert may make copies of information stored on any of the devices, subject to the following conditions. First, the Plaintiff must agree to the entry of an appropriate protective order that forbids the computer forensic expert from revealing to the Plaintiff (or anyone else) any of the information obtained from the Defendant's computer or devices that is not relevant to this action under FRE 401. Second, the protective order must forbid the computer forensic expert from retaining such information beyond the closing of this case, or permitting anyone else from retaining it. In addition, the Plaintiff will be required to pay any and all fees charged by the forensic expert during the investigation, but the computer forensic expert must agree to maintain his or her independence, rather than maintaining a client relationship with the Plaintiff.

Just to clarify to avoid any misunderstanding by Plaintiff's legal counsel, the Defendant is not trying to determine who the Plaintiff can have as its expert. The Defendant is only trying to prevent his personal and confidential information, that is wholly irrelevant to this action, from falling into the hands of the Plaintiff or its experts, while at the same time providing Plaintiff with everything it needs in a manner which the Plaintiff can rest assured that nothing was withheld.

Obviously the Defendant's desire is to not be subjected to annoyance, embarrassment, oppression, or undue burden or expense conflicts with the Plaintiff's desire to open and broad discovery (assuming the best intentions on the Plaintiff's part, rather than inferring a desire to impose an undue hardship on the Defendant). Fortunately, resolving such tensions and conflicts is exactly what Fed. R. Civ. P. 26(c) is for.

Irrelevant Information: the Defendant is not claiming that any of the information on his hard drive(s) that would support the Plaintiff's case is confidential. Rather, he is claiming that nothing on his hard drive will not be relevant to the Plaintiff's claims, and that such irrelevant information includes all of the private and confidential information that he wishes to remain private and confidential. If an independent expert determine that there is nothing on the Defendant's hard drive(s) in the nature of what the Plaintiff is seeking, the Plaintiff can hardly object to being precluded from discovering irrelevant information. Indeed, the United States Supreme Court has expressly held that, pursuant to Fed. R. Civ. P.26(b) relevancy is a *sine qua non* for information to fall within the scope of discoverability in the first place. See *Schlagenhauf v Holder,* 379 U.S. 104, 85 S. Ct. 234, 13 L. Ed. 2d 152 (1964). In this case the court's discussion of the "good cause" requirement of Fed. R. Civ. P.35(a) gave substaintial insight into the relevancy requirement of discoverability under Fed. R. Civ. P. 26(b)(1). That is, the Court noted that because the general scope of discovery is limited to any matter, not privileged, that is relevant to the subject matter of the litigation, then the "good cause" requirement of Rule 35(a) "would be meaningless if [it] could be established by merely showing that the desired materials are relevant, for the relevancy standard has already been imposed by Rule 26(b)." *Schlagenhauf, supra,* 379 U.S. at 117-118.

Financial Burden: the Plaintiff chose to bring this suit, and many like it, based solely on its claim that it can allegedly trace infringing activity to someone using (or appearing to use) the Defendant's IP address. Presumably, it must be aware that the correlation between the IP address and the user is somewhat loose, and that on many occasions it will have sued the wrong party. Apparently, it has determined that the financial gain it stands to realize through a broad application of that strategy outweighs the costs that it will incur (and impose) on those occasions where (as here) it has sued the wrong party. And of course, the cost of having the Defendant's hard drive(s) examined for evidence of file sharing is obviously one of the many contemplated costs of such a strategy.

In contrast, the Defendant did not sign up for any of this. He has been involuntarily dragged into this mess without ever installing or using BitTorrent to volitionally infringe on the Plaintiff's copyright, as the Plaintiff claims in this case.An independent forensic examiner, who is properly licensed in Pennsylvania, could provide the necessary information to both sides; it makes absolutely no sense for the Defendant to retain his own expert. Why pay for two experts, when one will do? Let the Plaintiff front the cost of a properly licensed and independent forensic examiner, and if the Plaintiff somehow prevails, it can always tax that cost as the prevailing party. But allow both the Defendant and Plaintiff to have equal access to the independent expert's report; this is the most fair and cost efficient method, and also the one that makes the most sense.

Licensing/Copyright Violations: as noted before, under Pennsylvania law, the investigator must be properly licensed to conduct the investigation required.To the extent that the Defendant's hard drive(s) contains authorized copies of other works that are subject to their own copyrights (such as computer programs legally purchased and licensed to the Defendant), the Plaintiff should be compelled to indemnify and hold the Defendant harmless for any

infringement of these copyrights, which would directly result from the imaging of his hard drive(s) that is required for this investigation.

CONCLUSION AND RELIEF REQUESTED

For the reasons stated above, Defendant seeks a protective order of this court under Fed. R. Civ. 26(c)(1) with regard to Plaintiff's request for a complete copy of the hard drive(s) on his computer. To wit:

Plaintiff and Defendant shall mutually agree upon the selection of an independent expert who is licensed in Pennsylvania. If Plaintiff and Defendant cannot agree on the selection of such an expert, then Defendant asks that the court appoint one from the nominees provided by the parties. Defendant will bring his computers and any other equipment within his custody and control and identified in these requests as being sought by Plaintiff for inspection at a mutually agreed upon time, where it/they can be examined by the independent expert in computer forensics:

- Said expert may make copies of the information stored on any of the devices mentioned above, subject to the following conditions.
  Said expert shall expressly agree to be bound by this protective order. Said expert will not real to Plaintiff (or any other person) any of the information obtained from Defendant's computer or other devices that is not relevant to this action under FRE 401.
- The parties will assist said expert in that regard by submitting to him or her mutually agreed upon interrogatories about the contents of Defendant's computer.
- The computer forensic expert must destroy and not retain, or permit anyone else (other than the Defendant) to retain information obtained from Defendant's computer after the case is closed.
- In addition, Plaintiff will be required to pay the computer forensic expert's fees, but the computer forensic expert must agree to maintain his or her independence, rather than maintaining a client relationship with plaintiff.

WHEREFORE, Defendant respectfully requests a protective order from this Court as set forth above.

DATED: *September 30th*, 2014

Respectfully submitted,

By: JDoe
John Doe
Pro se
johndoe69249@hushmail.com

CERTIFICATE OF SERVICE

I hereby certify that on 9/30/2014, I served a copy of the foregoing document, via US Mail, on:

Christopher P. Fiore, Esq.
418 Main St., Suite 100
Harleysville, PA, 19438

Dated: 9/30/2014

Respectfully submitted,

JDoe
John Doe
Pro se
johndoe69249@hushmail.com